The Final HIPAA Security Rule – A Quick Look

What’s Been Removed?

- Electronic signature standard
- Technical controls for networks including alarms and event reporting
- Certification per se. The idea of certification or accreditation has been replaced by *evaluation* of technical and non-technical controls.
- Requirement (in the Contingency Plan standard) for having available critical facilities for continuing operations in the event of an emergency.
- Formal mechanism for processing records. The requirement for policies and procedures to govern the handling of electronic health information has been removed. Some remnants of it can be found in requirements for data backup, device and media controls, and workstation security.
- Security configuration management, including asset inventory, hardware/software maintenance review, security features testing and virus checking. Virus checking has been reduced to procedures that are required under the security awareness and training standard.
- Personnel security (except the sanctions policy), including personnel security policy, maintenance of authorization records, supervision and training of technical maintenance personnel.
- References to potential solutions such as
  - role-based access and user-based access;;
  - penetration testing;
  - message authentication codes, checksums, double keying, digital signatures;
  - tokens, biometrics, PINS, telephone callback systems;
  - specific termination procedures, such as changing the combination locks, removal from access lists, removal of user accounts and turning in keys, tokens, or cards that allow access;
  - visitor sign-in and escorts, procedures for verifying access authorization.

What’s Changed?

- There is better synchronization of security with the privacy regulations in many areas, including definitions and rules for applicability, hybrid entities, affiliated entities and group health plans.
- The scope of the regulation is limited to ***electronic protected health information*** only.
- Approach is now risk management based rather than a list of mandatory controls. Covered entities must conduct risk assessments and perform risk analysis to determine risks and appropriate controls.
- *Requirements* have become *standards*. Compliance with standards is mandatory.
- *Implementation features* have become *implementation specifications*. Implementation specifications may be *required* or *addressable*. If required, compliance is mandatory. If addressable, the specification must be analyzed to determine if it is “reasonable and appropriate”. If it is reasonable and appropriate, it must be implemented. If not reasonable and appropriate, the rationale behind this decision must be documented, and

an equivalent alternative security measure must be implemented if reasonable and appropriate.

- Many previously *required* features are now *addressable*, e.g. determination of data and information criticality
- Training and security awareness training have been combined into a single standard. Covered entities are responsible for training only their own workforce. Training is not required for non-workforce system users.
- Encryption is an addressable solution for stored data as well as transmitted data. No distinction is made between data transmitted outside of the organization and data transmitted within the organization.
- Emergency mode operations plans are limited to business functions necessary to protect the security of the electronic protected health information.
- Electronic media has been expanded to cover more than just tapes and diskettes. It now includes hard drives, optical disk, digital memory cards, and transmission media, including the Internet, Extranets, leased lines, dial-up lines, private networks and the physical movement of removable/transportable electronic storage media.
- Requirements for business associate contracts or arrangements are spelled out. Business associates are requires to implement reasonable and appropriate security rather than specifically following the protections mandated in this final rule. Covered entities can require specific protection levels via the contract if both parties agree to it.

What’s Been Added?

- Security Standards: General Rules about:
  - what covered entities must do,
  - flexibility in the approach to securing the electronic protected health information
  - which requirements are mandatory and which can be addressed with alternative security measures,
  - when review and modification is needed.
- Organizational Requirements that address business associate contracts or arrangements.
- Policies and Procedures Requirements and Documentation Requirements that identify the rules for documentation, review, modification and retention of written policies, procedures, plans, contracts, etc.
- Requirements for isolating the clearinghouse function from the rest of the provider or health plan organization.
- Definitions for hybrid entity and affiliate
- Specific requirements for group health plans regarding plan documents and protection of ePHI by the plan sponsor.
- Sanitizing electronic media prior to making it available for re-use.
- Business associates are required to ensure that any agent, including a subcontractor, to whom it provides ePHI agrees to implement reasonable and appropriate safeguards. The business associate must also report any known security incident to the covered entity.
- Alternative arrangements in lieu of business associate agreements for government agencies.